SECURITY MECHANISMS WITH STEGANOGRAPHY

PROJECT WORK DONE AT

ER&DC

P-649

PROJECT REPORT

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF
MASTER OF ENGINEERING
OF BHARATHIAR UNIVERSITY, COIMBATORE.

SUBMITTED BY

SEENA.PS
Register Number 0037K009

GUIDED BY

EXTERNAL GUIDE

Ms.MANJIMA.S

INTERNAL GUIDE

Ms.SUGANTHI.N

Department of Computer Science &Engineering
KUMARAGURU COLLEGE OF TECHNOLOGY
COIMBATORE – 641 006
December 2001

DECLARATION

I here by declare that the project entitled "**SECURITY MECHANISMS WITH STEGANOGRAPHY**" submitted to **BHARATHIAR UNIVERSITY** as the project work of Master of Engineering (Computer science and Engineering) Degree, is a record of orginal work done by me under the supervision and guidance of **Ms.Manjima. S , *ER&DC*** and **Ms Suganthi.N , *Kumaraguru College of Technology*** and this project work done has found the basis for award of any degree/Diploma/Associateship/Fellowship or similar title to candidate of any university.

Place: Trivandrum
Date: 14/12/01

SEENA.PS

14/12/01
Internal Guide
Ms.Suganthi.N

External Guide
Ms.Manjima.S

Department of Computer Science &Engineering
KUMARAGURU COLLEGE OF TECHNOLOGY
(Affiliated to the Bharathiar university)
COIMBATORE – 641 006

CERTIFICATE

This is to certify the project work entitled

SECURITY MECHANISMS WITH STEGANOGRAPHY

Done by

SEENA.PS

Register Number 0037K009

Submitted in partial fulfillment of the requirements for the award of the degree of

Master of Engineering of Bharathiar University

Professor and Head
Dr.S.Thangasamy
20/12/'01

InternalGuide
Ms.Suganthi.N
14/12/01

Submitted for University Examination held on 20/12/01

Internal Examiner

External Examiner

R&DCI

भारतीय इलेक्ट्रॉनिकी अनुसंधान एवं विकास केन्द्र
(भारत सरकार सूचना प्रौद्योगिकी मंत्रालय
का स्वायत्त वैज्ञानिक संस्थान)
सॉफ़्टवेयर प्रशिक्षण एवं विकास केन्द्र
चेत्रांकरा बिल्डिंग,वेल्लयंबलम
तिरुवनन्तपुरम - 695 010, भारत
वेबसैट : www.erdcitvm.org

ELECTRONICS RESEARCH AND
DEVELOPMENT CENTRE OF INDIA
(An Autonomous Scientific Society of Ministry of
Information Technology, Government of India)
SOFTWARE TRAINING & DEVELOPMENT CENTRE
Chennankara Building, Vellayambalam
Thiruvananthapuram - 695 010, India
Website: www.erdcitvm.org

Phone: 0471-326531/326586/326012/322921 *Fax:* 0471-321209/ 331654/332230 *email:* stdc@erdcitvm.org

BONAFIDE CERTIFICATE

This is to certify that the project entitled **"SECURITY MECHANISMS WITH STEGANOGRAPHY"** using **Java 2**, is a bonafide record of the work done at the Centre by **Ms. SEENA P.S, Kumaraguru College of Technology, Coimbatore** in partial fulfillment of the requirements for the award of the **M.E (Computer Science)** degree from **Bharathiar University, Coimbatore.** She has been working on the project in the Centre during the period July 2001 to December 2001.

Certified further that to the best of my knowledge, the work reported herein does not form part of any other thesis on the basis of which a degree or award was conferred on an earlier occasion to this or any other candidate.

Saramma Chacko
Jt. Director

SOFTWARE TRAINING AND DEVELOPMENT CENTRE
A SCIENTIFIC SOCIETY OF THE MINISTRY OF INFORMATION TECHNOLOGY
ER & DC
GOVT. OF INDIA
T.C. 15/180-184
TRIVANDRUM
Pin-695 010

Manjima.S
Scientific Officer
(Project Guide)

Thiruvananthapuram
3-12-2001

ACKNOWLEDGEMENT

I would like to take this opportunity to express our deep gratitude to all the people who have helped and guided me in the various stages of this project

Firstly I thank the Lord Almighty for his immense grace and blessings at each and every stage of this project.

I acknowledge my gratitude to Ms. Saramma Chacko, Joint Director, ER&DC for permitting us to do the project and providing all facilities that made the experience a pleasant one.

I am extremely thankful to Dr. S.Thangasamy, Professor and Head of the Department for his kind suggestions he has given in every step through out our studies and in this project work.

I express my sincere thanks to Prof.K.R. Bhaskaran , Asst.Professor for his kind help and suggestions in every step through out the project

I express my sincere thanks to Ms Manjima.s , Scientific Officer for her valuable guidance and advice through out the course of the project work and also grateful to my internal guide Ms.Suganthi.N, Lecturer who offered her guidance and always supported me with keen interest and constant encouragement suggestions in every step through out the project

I would like to thank my parents who inspired us always .Without their encouragement I would never have gotten to where iam.

Iam thankful to all my teachers and non teaching staffs at the Kumaraguru college of technology for the help they gave me .

Lastly, I would like to thank my classmates and friends for their love and moral support.

CONTENTS

SYNOPSIS

The aim of the project is to develop a steganographic application for network security. Network security includes not just encryption but also traffic security, whose essence lies in hiding information. Steganography, an important part of information hiding, is the science of concealing a secret message within a "cover" message.

Project covers the steganographic method like hiding the information's under a cover text. It exploits the Steganographic Nature of whitespace. It conceals a secret message in ASCII cover text by appending spaces and tabs to the end of lines. Because spaces and tabs are invisible in most text viewers, the message is effectively hidden from casual observers.

Once a steganographic system is discovered, it is rendered useless. The problem can be recovered if the hidden data depends on some sort of key for extraction. Identity card is given to selected users along with the password(key).

The password is embedded in the photo of an identity card and a user who holds original id card can view the secret message under a cover text by going through a login password sequence. The user password is verified with the password embedded in a photo and if password matches, the message can be extracted.

Hiding arouses less suspicion to the users. Password embedded photo enforce ownership and also duplication of the card is prevented. This type of marks in a secret fashion to enforce ownership, uses Watermarking system, another important part of information hiding.

INTRODUCTION

1.1 PROJECT OVERVIEW

This project is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers if encryption is used, message cannot be read even if it is detected.

Once a stenographic system is discovered, it is rendered useless. The problem can be recovered if the hidden data depends on some sort of key for extraction. Identity card is given to selected users along with the password (key).

In the field of data security, the password is hidden as an invisible watermark in the photo of the card. If anyone would intend to counterfeit the passport by replacing the photo, it would be possible to detect the change by scanning the passport and verifying the password hidden in the photo, does not match any more with the user login password. If it matches then user can view the message.

1.2 ORGANIZATION PROFILE

ER & DC a national center of Excellence in Electronics Research and Development is an autonomous Scientific Society under the Department of Electronics, Govt. of India, doing Application Oriented Research and Development in high-tech areas in Electronics and Information Technology. The center at Thiruvananthapuram was originally started in 1974 under Department of Science and Technology and was subsequently taken over by Department of Electronics via Gazette notification dated May 6th, 1988 and has completed ten years as a center for Applied Electronics and Research and Development of Electronics. It is a pioneer organization in India engaged in application, technology, catering to the needs of industry, defense and service sections of the country.

ER & DC, have been providing services to practically all Govt. departments as well as private organizations. It has established several information systems database on various socio-economic areas.

Objectives of ER&DC

- To undertake research and development in the area of applied electronics for rural applications.
- Research and Development support to industries in the region, both in public and private sectors.
- Development of electronics products and systems for manufactures in small-scale sectors.
- To play the model role in the development of electronic technology in the region.

There are five ER&DC located in our country each has own specific research design.

- Calcutta
- Lucknow
- Mohali
- Pune
- Trivandrum.

STDC

Software Training and Development Centre (STDC), is the software development center under ER&DC. Software development has been identifies as a major thrust area of the center. The center concentrates on meeting the software development requirement of major industrial and other establishment, software manpower development, support to software export etc.

The Software training and Development center (STDC) of the Electronics Research and development Centre of India. Thiruvananthapuram, has been the premier organization in Computer Education. The courses are offered at Software Training and development Centre (STDC) Trivandrum and Kochi. ER&DCI is an Authorized training partner of IBM Global services for Mainframe Education. It is also recognized as Authorized Training center by ORACLE SOFTWARE INDIA for conducting Oracle Education Career Programme.

Objectives

- The build highly effective and skilled software professionals, to provide education and service to customers to meet their needs.
- To run high quality business educational services.
- To be leader in technology and productivity relation to computers.

The Trivandrum center has transferred technologies to several manufactures and also undertaken new projects in the area of

- Frame relay interface
- News-room Automation
- Artificial Intelligent Tools
- Speech I/O cards.

1.3 STEGANOGRAPHY

The word steganography comes from the Greek *steganos* (covered or secret) and -*graphy* (writing or drawing) and thus means, literally, covered writing. Steganography is usually given as a synonym for cryptography but it is not normally used in that way. Through recent usage, steganography has come to mean hidden writing, i.e., writing that is not readily discernible to the casual observer.

In an ideal world we would all be able to openly send encrypted email or files to each other with no fear of reprisals. However there are often cases when this is not possible, either because you are working for a company that does not allow encrypted email or perhaps the local government does not approve of encrypted communication (a reality in some parts of the world). This is where steganography comes to play.

Steganography simply takes one piece of information and hides it within another. Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside of them. An image of the space shuttle landing might contain a private letter to a friend. A recording of a short sentence might contain your company's plans for a secret new product. Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, microdots, digital signatures, covert channels and spread-spectrum communications. Today, steganography is used on text, images, sound, signals, and more. To place a hidden "trademark" in images, music, and software, a technique referred to as watermarking.

Perhaps when you were a child, you used lemon juice to write text on paper, then let the paper dry. Your writing would miraculously reappear on the

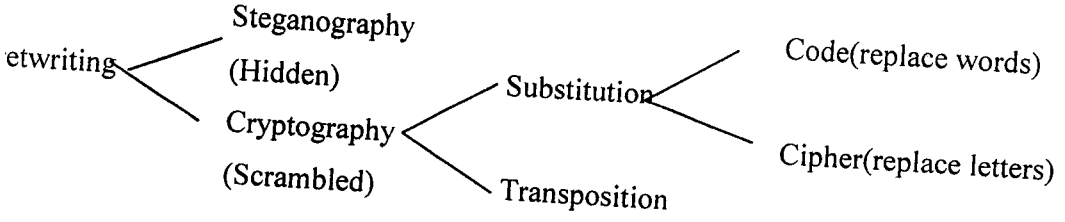
apparently blank sheet of paper when you heated it. Or perhaps when you were older, and were introduced to money, you noticed the image, or watermark, that would appear on bank notes when they were held up to the light. Both these types of situations are examples of steganography, the art of secret writing.

``the goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present."

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide.

In fact, it is common practice to encrypt the hidden message before placing it in the cover message. However, it should be noted that the hidden message does not need to be encrypted to qualify as steganography. The message itself can be in plain English and still be a hidden message. However, most steganographers like the extra layer of protection that encryption provides. If your hidden message is found, then at least make it as protected as possible.

However, steganography has a number of disadvantages as well. Unlike encryption, it generally requires a lot of overhead to hide a relatively few bits of information. However, there are ways around this. Also, once a steganographic system is discovered, it is rendered useless. This problem, too, can be overcome if the hidden data depends on some sort of key for extraction.



1.4 WATERMARKING

Digital watermarking provides a means of embedding a message in a piece of digital data without destroying its value. Digital watermarking embeds a known message in a piece of digital data as a means of identifying the rightful owner of the data. These techniques can be used on many types of digital data including still imagery, movies, and music. This paper focuses on still digital.

Digital watermarking provides the owner of a piece of digital data the means to mark the data invisibly. The mark could be used to serialize a piece of image it is used as a method to enforce the ownership and prevents the duplication of the particular image, For example, this marking allows an owner to safely use an ID card for verifying but legally provides an embedded copyright to prohibit others from using the same .

Watermarks and attacks on watermarks are two sides of the same coin. The goal of both is to preserve the value of the digital data. However, the goal of a watermark is to be robust enough to resist attack but not at the expense of altering the value of the data being protected. On the other hand, the goal of the attack is to remove the watermark without destroying the value of the protected data.

Images have an advantage over other pieces of digital data such as a word processed document. The contents of the image can be marked without visible loss of value or dependence on specific formats. For example a bitmap (BMP) image can be compressed to a JPEG image. The result is an image that requires less storage space but cannot be distinguished from the original. Generally, a JPEG level of 7 (70%) or higher can be applied without humanly visible degradation. This property of digital images allows insertion of additional data in the image without altering the value of the image. The message is hidden in unused visual space on the image and stays below the human visible threshold for the image.

1.5 THE CURRENT STATUS

The major direction in steganography is the technique of hiding messages in innocuous computer files such as digital pictures and digitized audio. For example, the least significant bits of a bitmap graphic can be used to hide messages. The message is contained in the least significant bits and changing these bits causes an almost imperceptible change in the bitmap image itself. Without a direct comparison of the original and the processed image, it is practically impossible to tell that anything has been changed. . Using these techniques, it is possible to send a secret message to someone who knows and no one else will even know that the message is there. In digitized audio files, By encoding the message in the least significant bits of a wave file, for example, the message is hidden and, again, it is almost impossible to detect that anything in the wave file has changed. Another method is to hide messages in the unused sectors of a floppy disk.

Now Steganography is destined to become more important as more people join the Cyberspace revolution and as the existing governments of the world attempt to regulate or prohibit the use of cryptography for personal privacy purposes. If the government prohibits the use of cryptography, you can still send encrypted messages by hiding the encrypted message in another innocuous file using steganographic techniques. And thus another statist attempt to control Cyberspace can be thwarted by technology.

Watermarking refers to hiding some sort of signature within an image/video/sound datafile to establish traceable ownership of the data. Many projects for the development and analysis of watermarking techniques for audio, images, and video data are under development stage to meet certain criteria such as (1) nondestructability by various processes, (2) nondetectability, (3) minimum distortion, and or (4) minimum overhead. Recently developed a new music watermaking techniques with excellent robustness qualities.

1.6 RELEVANCE AND IMPORTANCE OF THE TOPIC

Throughout history, people have been hiding information by employing several methods. Putting aside the examples from the world of espionage, steganography can be very useful in real world applications. One of these could be the transmission of credit card numbers through the Internet, where ciphered data act like a magnet for hackers. With steganography, the existence of sensitive information is not even noticed.

Another scenario for its utilization is when it is desired to maintain certain information hidden within an organization, avoiding the risk of being taken by disgruntled employees. Also, when it is desired to manage confidential information without knowledge of the secretary or the assistant; or when it is desired to send a boss, a colleague or a subordinate some information "just for your eyes".

The main difference between *watermarking* and *steganography* basically lies on the intention. Traditionally, the latter hides information, whereas watermarking extends the information and becomes an attribute of the sealed document. In steganography, the object of communication is the hidden message, and the "packaging" is only a means of sending it. In watermarking, the object of communication is the packaging and the hidden message only references that packaging.

Watermarking techniques may be relevant in the following application areas First applications that came to mind were related to copyright protection of digital media. In the past duplicating artwork was quite complicated and required a great expertise for that the counterfeit looked like the original. However, in the digital world this is not true. For everyone it is extremely easy to duplicate digital data and this even without any loss of quality. Similar to the process in which artist artistically

signed their paintings with a brush to claim their copyrights, artists of today can watermark their work and hide for example their name in the image. Hence, the embedded watermark will allow identifying the owner of the work. It is clear that this concept is also applicable to other media such as digital video and audio.

The distribution of digital audio over the Internet in the MP3 format is currently a big problem. In this scenario digital watermarking may be useful to set up a controlled audio distribution and provide efficient means for copyright protection.

There is a number of possible applications for digital watermarking technologies and this number is increasing rapidly. For example, in the field of data security, watermarks may be used for certification, authentication, and conditional access. Certification is an important issues for official documents, such as identity cards or passports.

Digital watermarking allows to mutually link information on the documents. That means that some information is written twice on the document: for instance, the name of a passport owner is normally printed in clear text and is also hidden as an invisible watermark in the photo of the owner. If anyone would intend to counterfeit the passport by replacing the photo, it would be possible to detect the change by scanning the passport and verifying the name hidden in the photo does not match any more the name printed on the passport.

Similar to standard paper watermarks, digital watermarks can also be used to watermark white paper with the goal to authenticate the originator, verify the authenticity of the document content, or date the paper. Such applications are especially of interest for official documents, such as contracts. For example, the watermark can be used to embed the name of the lawyer or important information such

as key figures. In the event of a dispute the watermark can be read and allows the authentications of key information in the contract.

Another application is the authentication of image content. The goal of this application is to detect alterations and modifications in an image.

Other applications related to conditional access and copy-control are also possible. For example conditional access to confidential data on CD-roms may be provided using digital watermarking technology. The concept consists of inserting a watermark into the CD label. In order to read and decrypt the data stored on the CD, the watermark has to be read since it contains information needed for decryption. If someone copies the CD, he will not be able to read the data in clear-text since he does not have the required watermark. To read the data on the CD, the user starts a program on the CD. This program asks the user to put the CD on the scanner and then reads the watermark. If the watermark is valid the program decrypts the data on the CD and gives the user access the clear-text data.

A different application is related to copy-control. Several companies work on a watermarking system for copy control in the DVD environment. Fully functioning solutions exist already, however, for the moment they have not been entirely approved by the content producers and providers. Finally, this solution is also an efficient and simple way to prevent the use of illegal copies of software. It has a similar functionality as the anti-piracy device called "dongle", but is more compact (you can loose a dongle) and less expensive.

Watermarks are not particularly effective in assuring data integrity, in that they are usually resilient only to small changes in the data object (cropping, tone-scale correction) and are invalidated by large changes (such as the removal of a figure from an image). Indeed, there is some doubt whether any data-hiding technique will be

sufficient for an application that requires data integrity. In cases where proof of data integrity is required, only PKCS mechanisms, which are intolerant of any transformation of the marked object, will provide this level of security.

In medical field, watermarks convey object-specific information (" feature tags" or " captions") to users of the object. For example, individual features in a still image might be labelled, and the whole image given a caption. This may be used to attach patient identification data to medical images, or to highlight regions of diagnostic significance. These applications require relatively large quantities of embedded data. While there is no need to protect against deliberate tampering, normal use of the data object may involve such transformations as image cropping, or scaling, and will require the use of a technique that is resistant to those types of modification.

Different techniques may be required according to the type of media (audio, image, video), and the encoding format used. In addition, each applications area may require different technologies to address the specific service requirements of that area. Finally, further choices may be made depending on the types of transformation (e.g. the compression algorithms) the object is likely to encounter.

LITERATURE SURVEY

IEEE Spectrum May 2000 Volume 37 Number 5

Hiding data

Abstract:

A more modern application is the digital watermark, for identifying official copies of copyrighted images and recordings. Unlike encryption, which hides the content of a message in an obvious manner, steganography hides the mere existence of anything hidden. This volume reveals some of computer-based steganography programs popular today ,based on 3 techniques and some of the commercial steganography software tools

- Merging the information to be hidden into a "cover" sound file by changing the least significant bit of each digitized sample of the file. The resulting file sounds the same to the human ear and is the same length as the original file.
- Merging the information to be hidden into a cover image file by changing the least significant bit of the digitized value of the brightness of each pixel. Typical images use 256 levels of brightness, with 8 bits per pixel for black-and-white images and 8 bits for each of the three primary colors (red, green, and blue) per pixel for color images.

Hiding data in the areas of a computer floppy disk or hard drive that are normally not accessed. A computer disk is divided into clusters, each of which holds from 512 bytes to over 32 000 bytes. When a file is saved, it uses a portion of one or more clusters; because DOS and Windows store only one file per cluster, the space left over between the end of a file and the end of the cluster (called the slack) is available to hide data in. This scheme is extremely easy to detect, however.

The most commonly used commercial steganography software tools are Hide and Seek, Steganos, StegoDos, White Noise Storm, S-Tools for Windows, Jpeg-Jsteg, and Stealth. For Unix computers, there is SFS (Steganographic File System).

Law enforcement agencies treat steganography much like a computer virus: once a program hits the market in a big way, tools are developed to detect it. The more extensive the program's use, the more resources are devoted to detecting its footprint.

An Information-Theoretic Approach to the Design of Robust Digital Watermarking Systems

Authors:**BrianChen, Gregory W Wornell,** Page (NA) Paper number 3007

Abstract:

A variety of emerging applications require the design of systems for embedding one signal within another signal. We describe a new class of embedding methods called quantization index modulation
(QIM) and develop a realization termed coded dither modulation in which the embedded information modulates the dither signal of a dithered quantizer. We also develop a framework in which one can
analyze performance trade-offs among robustness, distortion, and embedding rate, and we show that QIM systems have considerable performance advantages over previously proposed spread-spectrum and low-bit modulation systems.

Authors: **MinWu,MattL.Miller,JeffreyA.Bloom, A"Ingemar J Cox**, Page (NA) Paper number 3008.

Abstract:

Watermarking algorithms that are robust to the common geometric transformations of rotation, scale and translation (RST) have been reported for cases in which the original unwatermarked content is available at the detector so as to allow the transformations to be inverted. However, for public watermarks the problem is significantly more difficult since there is no original content to register with. Two classes of solution have been proposed. The first embeds a registration pattern into the content while the second seeks to apply detection methods that are invariant to these geometric transformations.

This paper describes a public watermarking method which is invariant (or bares simple relation) to the common geometric transforms of rotation, scale, and translation. It is based on the Fourier-Mellin transform which has previously been suggested. We extend this work, using a variation based on the Radon transform. The watermark is inserted into a projection of the image. The properties of this projection are such that RST transforms produce simple or no effects on the projection waveform. When a watermark is inserted into a projection, the signal must eventually be back projected to the original image dimensions. This is a one to many mapping that allows for considerable flexibility in the watermark insertion process. We highlight some theoretical and practical issues that affect the implementation of an RST invariant watermark. Finally, we describe preliminary experimental results.

If One Watermark is Good, Are More Better?

Authors: ***FredMintzer,Gordon W Braudaway,*** Page (NA) Paper number 3009

Abstract:

Invisible watermarks are not all alike. Different techniques are used to embed different types of watermarks into digital media objects to accomplish different goals. Some watermarks are intended to robustly carry ownership information; some are intended to carry content-verification information; and some are intended to convey side information, or captions. In this talk, some opportunities to employ multiple watermarks to convey multiple sets of information, intended to satisfy differing or similar goals, are examined. Problems presented by the insertion of multiple watermarks are discussed. Progress towards developing techniques that embed multiple watermarks into an image will also be presented.

Detecting Electronic Watermarks in Digital Video

Authors:***Jean-PaulLinnartz,TonKalker, Jaap Haitsma,***Page (NA) Paper number 3010

Abstract:

Electronic watermarking is an active area of research with many applications being foreseen. Watermarks may be come an essential tool for copy management in future Consumer Electronic or PC devices. With simple circuits, detection of watermarks after noise addition, MPEG compression, D/A conversion, pixel shifts appears feasible, but detection after transformations, such as cropping and stretching, remains a challenge. We propose a model to evaluate the effect of scaling on the detector reliability and verify it with experiments.

Data Embedding in Audio: Where Do We Stand

Authors: ***AhmedHTewfik,MitchellDSwanson,Bin Zhu,***Page (NA) Paper number 3011

Abstract:

Data embedding algorithms embed binary streams in host multimedia signals. The embedded data can add features to the host multimedia signal or provide copyright protection. We review requirements for transparent data embedding techniques in audio signals. We describe and contrast current approaches to data embedding in audio. In particular, we emphasize the advantages and limitations of the various approaches. we also describe possible signal processing and protocol level attacks on audio watermarking algorithms. We conclude with a discussion of future research directions.

The Business Case for Audio Watermarking

Authors: ***Paul Jessop,*** Page (NA) Paper number 3012

Abstract:

This presentation will review the applications of audio watermarking for the recording industry. It will examine the reasons for placing watermarks in sound recordings, the benefits which might result and the potential hazards which need to be overcome. It will cover the objectives, methodology and results of the MUSE project, one of whose tasks was the evaluation of ``embedded signaling'' systems. Finally, it will look at recent developments in the adoption of watermarking in the recording industry.

Dr. Martin Kutter and Dr. Frédéric Jordan

http://www.jtap.ac.uk/reports/htm/top

This article serves as an introduction to digital watermarking, the main fields of applications, and some practical examples of software implementations using this technology. Digital watermarking is an adaptation of the commonly used and well-known paper watermarks to the digital world. Digital watermarking describes methods and technologies that allow hiding of information, for example a number or text, in digital media, such as images, video and audio. The embedding takes place by manipulating the content of the digital data, that means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark has to be robust or fragile, depending on the application. With robustness we refer to the capability of the watermark to resist to manipulations of the media, such as lossy compression, scaling, and cropping, just to enumerate some. Fragility means that the watermark should not resist tampering, or only up to a certain extent.

Overview of Watermarks, Fingerprints, and Digital Signatures

SandyShaw
The University of Edinburgh

This paper presents a technical analysis of the capabilities and characteristics of technologies proposed for use as a means of providing copyright protection for digital information resources:

a) Watermarks and fingerprints provide indication of ownership, and indication of the identity of a licensed user, respectively, by embedding security information in the digital object. This information may be visible (as in a backwash image), or, more conventionally, invisible. While this has some attraction to copyright owners, the security properties of this technology are limited.

b) 'Digital signatures' is a popular term for one of the capabilities of public key cryptosystems (PKCS). As well as providing signature services (origin authentication), this technology supports content confidentiality and content integrity services. These services are reliable ('strong' in the terminology of cryptography), but the technology is not designed for use in environments where data objects are subject to modification (e.g. by compression). Moreover, its deployment would be likely to incur a significant cost.

The paper also considers developments in US law, concerning the digital information environment, which may influence developments in European law, and affect commercial practice for providing access to digital information resources.

Steganographic Watermarking for Document

Benjamín Barán
Centro Nacional de Computación
Universidad Nacional de Asunción

Víctor Bogarín
Computer Science Department
RMIT University

Santiago Gómez
Centro Nacional de Computación
Universidad Nacional de Asunción

Abstract

The present paper defines Digital Seals for Documents, their scope, application environment and limitations. These seals can be used to insert information on documents, as with watermarking, or to use documents as a communication channel for sending concealed messages, as it is the goal of steganography. Users can decide to employ one, another functionality, or a combination of them depending on their needs or preferences.

Towards these objectives, a system was developed which constitutes a kit with several Sealing options. The system writes either visible or invisible marks in digital documents, following different methods designed and created in this project. These marks or seals, in turn, can be viewed through a Seal Recognizer. Implementation is done on RTF (Rich Text Format),which is a commercial, massively accessible format.

ENVIRONMENT PROFILE

1. JAVA

The Java language provides a number of important features that make it the language of choice for enterprises applications. The language is portable. It is object-oriented (in fact, there is no other way to write a program but as an object-oriented program). It provides a run-time environment that creates a security layer between the application and the client machine. And the language provides easy access to a number of important features. The following section identifies and explains some of these features.

The Java Runtime Environment

The Java application runs in a runtime environment known as the Java virtual machine. The Java virtual machine consists of an interpreter that reads and interprets the byte codes that make up the application. This interpreter dynamically loads classes as they are needed. Additional portions of the virtual machine perform garbage collection, freeing memory when it is no longer needed, and managing other resources.

This architecture provides platform transparency for the application. The Java programmer need not be concerned with porting issues; these issues are solved by the Java virtual machine. As long as the Java programmer writes to the Java portable libraries, the application is portable.

Language Safety

The Java language succeeds on many levels. It is powerful, yet safe, language. It Provides platform independence. It has built-in Web functionality. It uses a familiar

C/C++ language syntax. It provides easy language access to its multi-threading support.

It is portable.

Object-Oriented

Java was designed to be easy for the professional programmer to learn and use effectively. If you already understand the basic concepts of object-oriented programming, learning Java will be even easier. Object-oriented programming is at the core of Java. Java provides mechanisms that help you implement the object-oriented model. They are encapsulation, inheritance, and polymorphism. Encapsulation is the mechanism that binds together code and the data it manipulates, and keeps both safe from outside interference and misuse. Inheritance is the process by which one object acquires the properties of another object. Polymorphism is a feature that allows one interface to be used for a general class of actions.

The multiplatformed environment of the Web places extraordinary demands on a program, because the program must execute reliably in a variety of systems. Thus the ability to create robust programs were given a high priority in the design of Java. To gain reliability, Java force to find mistakes early in program development. Java was designed to meet the real-world requirement of creating interactive, networked programs. To accomplish this, Java supports multithreaded programming. Java is designed for the distributed environment of the Internet, because it handles TCP/IP protocols. Programs carry with them substantial amounts

of run-time type information that is used to verify and resolve accesses to objects at run time.

Java Advantages

- Immediate Demonstration on Web
- Built-In Graphics Rendering
- Image and ImageFilter Classes
- Portable

Java Disadvantages

- Slow (Interpreted Byte-code)
- No High Level Mathematics
- No symbolic manipulation

FRAME

A Frame is a top-level window with a title and a border. The size of the frame includes any area designated for the border. The dimensions of the border area can be obtained using the getInsets method, however, since these dimensions are platform-dependent, a valid insets

value cannot be obtained until the frame is made displayable by either calling pack or show. Since the border area is included in the overall size of the frame, the border effectively obscures a portion of the frame, constraining the area available for rendering and/or displaying subcomponents to the rectangle which has an upper-left corner location of

CANVAS

A Canvas component represents a blank rectangular area of the screen onto which the application can draw or from which the application can trap input events from the user.
An application must subclass the Canvas class in order to get useful functionality such as creating a custom component. The paint method must be overridden in order to perform custom graphics on the canvas.

IMAGES

As image communications systems and multimedia broadcasting systems are more and more frequently used today, it is necessary to develop suitable mechanisms for accessing images. Images offer the best way to work with Java graphics; as a matter of fact, everything in the AWT seems centered on the concept of images.

Displaying Images

Images are nothing more than a collection of colors and their layout, but they are useful because, with an auxiliary paint program, you can create sophisticated visual effects that can be captured and displayed in your application. Java arrives with built-in support for two types of images: GIF and JPEG. The GIF standard (Graphics Interchange Format)

is maintained by CompuServe. It uses an excellent compression scheme (LZW) to represent a large image in a small file. JPEG (Joint Photographic Experts Group) is an international standard mainly used for photographic material. It uses a discrete cosine transform (DCT) to remove extraneous material your eye doesn't really notice, so a very efficient compression scheme can be used. The cosine transform is "lossy," meaning it loses some information when applied. LZW, on the other hand, is "lossless." It turns out that the information removed by a cosine transform is precisely the photographic detail that your eye does not see.

Comparison of GIFs and JPEGs

Color depth

The maximum number of colors that a graphic can display is a function of it's *color depth*, which is an integer that designates how many bits of memory are used to code for the color of each pixel. Number of colors is equal to 2 raised to the power of the color depth. For example, an image with a color depth of 5 bits per pixel can have, at most, 2x2x2x2x2=32 colors

GIF and JPEG color depth

A GIF can be stored with a color depth of 1 bit per pixel (a maximum of 2 colors in the image) up to a depth of 8 bits (256 colors). A new GIF standard that will enable a depth of 24 bits.

JPEGs are always either 8-bit, enabling up to 256 greyscales, or 24-bit, enabling up to 16 777 216 colors, the 24- bit flavor being far more prevalent. color combinations and a single JPEG is capable of displaying it all at once, although in practice, any given JPEG will use

only a fraction of its palette.

GIFs, because they are 8-bit at most, and their palettes are chosen from a 24-bit "super-palette," cannot use all 16 million colors. However, they can easily display all of the colors in their reduced palette of 2 to 256 colors.

Loading Java Images

Both these formats can be easily loaded by your applets:

ImagenewImage=getImage(*URL*);
Image newImage = Toolkit.getDefaultToolkit().getImage(*filename or URL*);

The first line may be used only from a subclass of Applet, but line two can be called by either an applet or application. Each getImage() method returns immediately, without actually loading the image. To retrieve the image, you must try to display it; this is done to keep memory consumption down. For example, sometimes an applet might refer to an image, but not actually make use of it. Therefore, until the image is really needed, it will remain on the server.

Image Display

Once an Image object is instantiated, it can be displayed in an applet's paint( ) method by using the Graphics object passed to it:

g.drawImage(newImage, x, y, this);

Variables x and y contain the coordinates of the image's upper-left corner, and the final parameter is an ImageObserver object. This interface is implemented in the Component class that the applet is derived from, which is why you can pass the this pointer.

Tracking Images

Image loading can also be tracked by using the MediaTracker class. It will not call back when something completes. The client of a MediaTracker object must register images with the tracker, then ask for status. *Registration* involves passing an image and assigning a tracking number to it, which then is used to query for the image's status. The following methods are available for image registration:

- public void addImage(Image image, int id);

Java Color models

An image is a collection of colors and their layout. Humans perceive color when combinations of wavelengths of visible light stimulate the retina. The number of wavelength combinations is infinite, but humans can see only a fixed subset as separate colors. Therefore, *color models* were invented to group human-visible colors into a working set. There are two predominant color models used to represent color information:

- The CMY (cyan-magenta-yellow) color model is used in subtractive color systems, such as printing.
- The RGB (red-green-blue) color model is used in additive color systems, such as television and computer screens.

Printing is a *subtractive system* because the perceived color is contained in wavelengths of light reflected from the paper. The absorbed colors are said to be "subtracted" from the perceived color. Conversely, an *additive color system* creates the light source containing the color. Therefore, you can watch television in the dark, but you can't read a magazine.

Default RGB

Java uses the RGB color model for all its painting; all other models are eventually translated into this format. It has 8 bits of red, 8 bits of green, 8 bits of blue, and 8 bits of alpha. The alpha channel supplies transparency-255 is opaque (visible), and 0 is transparent. These add up to 32 bits of color information, which just happens to be the size of a Java integer. The format of colors within an integer is 0xAARRGGBB.

To support images, Java supplies two other ColorModels: DirectColorModel and IndexColorModel.

Direct Color

The DirectColorModel is used when the underlying pixels in an image contain the RGB values directly. This is also known as "true color." There are two constructors-one with an alpha channel, one without. To create the model, you need to specify only the number of bits per pixel and which bits correspond to which color:

Index Color

The IndexColorModel is used when the underlying pixels in an image represent an index into a color table. Most bitmaps fall into this category because the actual colors are contained in a color map somewhere in the file. The actual pixel data represent indexes into the color map instead of complete RGB values.

MemoryImageSource

ImageProducer class contained in Java.awt.image that creates a new image from an array of data .constructors used MemoryImageSource (int *width,* int *height*, int *pixel[ ],* int *offset*, int *ScanLineWidth*)

PixelGrabber

The PixelGrabber class is defined within Java.lang.image. It takes an existing image and grabs the pixel array from it.First create an int array big enough to hold the pixel data, create a pixelGrabber instance passing in the rectangle that want to grab. Finally call grabPixels() On that instance.

PixelGrabber(Image *imgObj*, int *left*, int *top*, int *width*, int *height*, int *pixel[ ]*, int *offset*, int *ScanLineWidth*)

SYSTEM STUDY & ANALYSIS

4.1 PROPOSED SYSTEM

The proposed system **"SECURITY MECHANISMS WITH STEGANOGRAPHY"** is a Steganographic application for network security, embedding secret information in an ASCII cover text by appending spaces and tabs to the end of lines. Because spaces and tabs are invisible in most text viewers, the message is effectively hidden from casual observers. Information embedded texts are created and saved by the creator later the users can use login password for verifying with the password embedded in a photo of the identity card. If it satisfies information can be viewed. This is used for sending messages between a defense contractor or to a spy. It arouses less suspicion for others.

EXTERNAL INTERFACE REQUIREMENTS

User Interface

The system should present an on screen interface for entering data into the system.

Software Interface

The system is developed using Java.

Hardware Interface

Any IBM compatible PC with atleast 64MB RAM .

Error Messages

Appropriate error messages will be displayed whenever necessary.

DESIGN CONSTRAINTS

Software Constraints:

Operating System : Windows95/98

Language used : Java2.0

Hardware Requirements:

System Processor : Pentium II processor

Speed: 350MHz

Hard disk: 10GB

RAM: 64MB

4.2 SYSTEM DESIGN

PROPOSED LINE OF ATTACK

Once a steganographic system is discovered, it is rendered useless. Software is now available to alter the extra information stored in files, making it possible to test the robustness of watermarking technologies and to detect and destroy stego'd information. Researchers are making progress in blind steganalysis techniques to detect messeges in carrier files without knowing the underlying technique.

- Steganalysis – the art of discovering steganographic data and rendering it useless

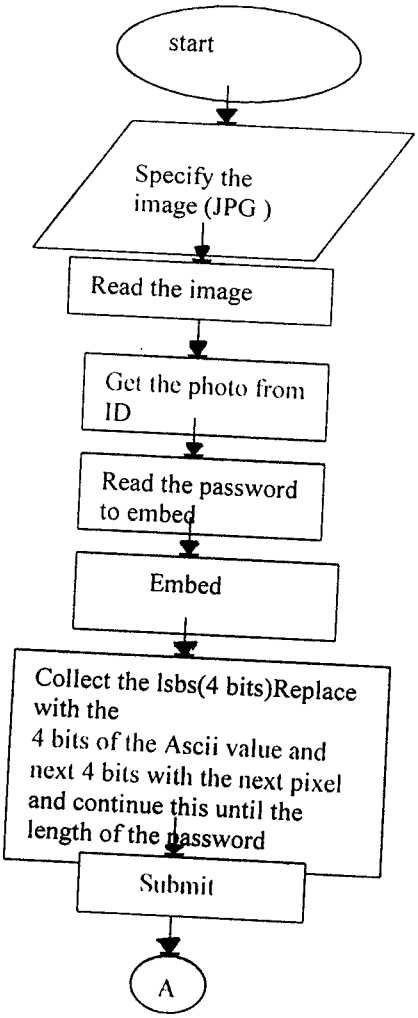
Steganography Detection & Recovery Toolkit (S-DART) – Air Force Research Laboratory sponsored program to develop algorithms and

- techniques for detecting steganography in computers and electronic transmissions

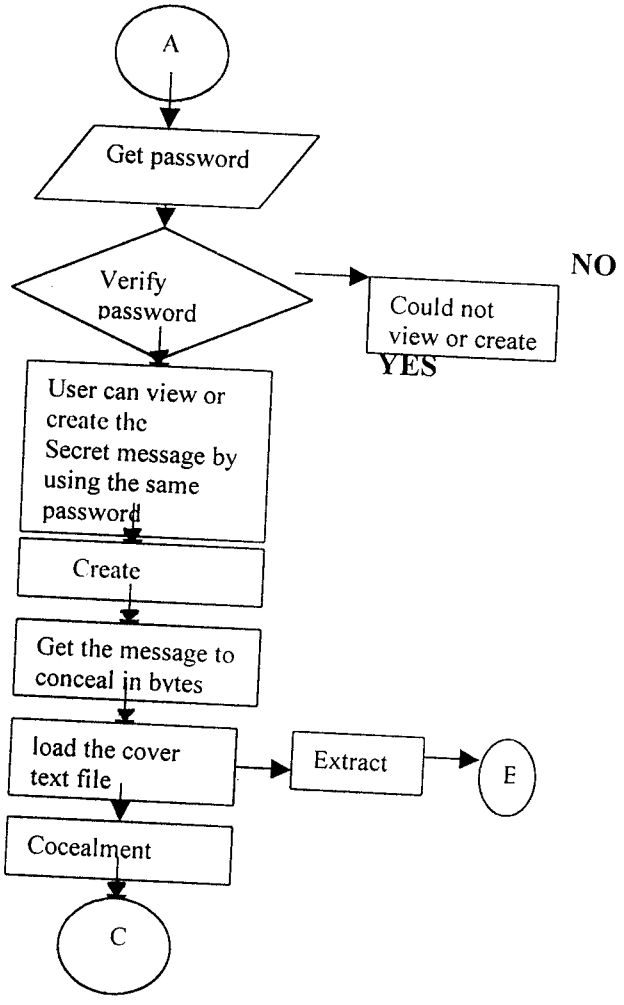
- Secret Messages Come in .Wavs – WIRED article by Declan McCullagh detailing current research to uncover concealed messages embedded in sound and video files
- Stegdetect – tool for detecting steganographic content in JPEG images hidden by Jsteg, JP Hide and Seek, and older version of Outguess
- Watermarking Software – copywrite protect digital images, music, and software with this stego technique
- Watermarking Weakness – discusses attacks on the current software
- Unzign and Stirmark – remove watermarks from many popular programs
- 2Mosaic – disables watermarks in jpg's by imperceptibly cutting the image into a number of smaller subimages

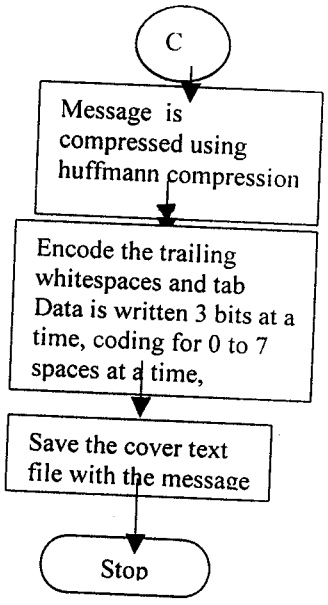
4.3 FLOWCHARTS

EMBEDDING THE MARK ON THE PHOTO

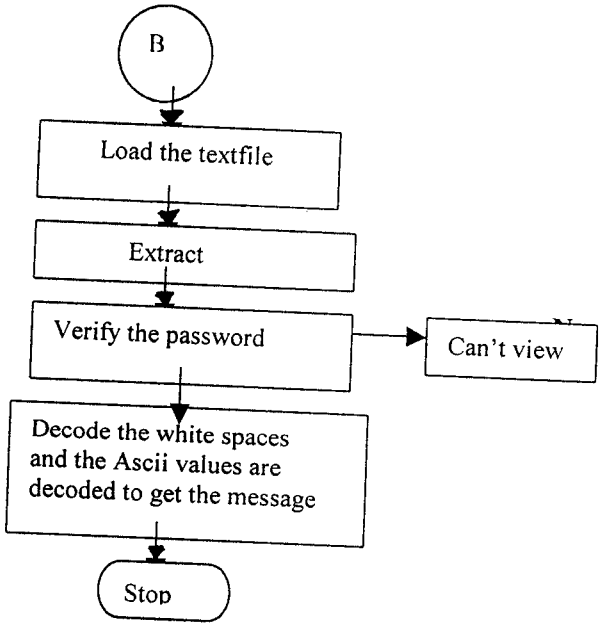


EMBEDDING THE MESSAGE UNDER A COVERTEXT





VIEWING THE SECRET MESSAGE



4.4 PROGRAM DESCRIPTION

FEATURES

Image types : Two formats GIF and JPEG can be accessed with this program

Password : Ascii format

Hiddentext :Ascii format

Compression :Huffmann compression algorithm

Covertext :Ascii format

This system implements

1.Stegimage

Concepts

Embed:

Technique inserts the password in the last four least significant bits of the image. This allows a watermark to be inserted in an image without

affecting the value of the image.

Extract:

Technique extract the bits from the LSB bits of the image and combine to form the password

2.Mycanvas

This extends the canvas class to encapsulates a blank window upon which we can draw.

3.Stegencode

It is a class for concealing messages in text files by appending tabs and spaces on the end of lines, and for extracting messages from files containing hidden messages. Tabs and spaces are invisible to most text viewers, hence the steganographic nature of this encoding scheme.

Embed:

Embed each character of the secret message in the form of trailing whitespaces of the cover text.

Extract:

Decode message the whitespaces and extract the secret message

4.Stegcompress

The compression scheme used by "Stegcompress" is a fairly rudimentary Huffman encoding scheme, where the tables are optimised for English text.

INPUTS

Submit frame:

Embed Password : Password to embed into an identity photo

User frame:

Password: Password to enter into the application

Embed frame &Extract frame

Hidden_text: Secret information to be hidden

Cover_text: Cover message to embed the message

Password_field : Password to extract the secret information

OUTPUT

Password is hidden as a watermark in the identity photo and extracted for verification with the user password. Secret message is

encoded as trailing whitespaces in a cover message and viewed later for the selected users.

4.5 DETAILED DESCRIPTION

Details of the proposed system

Steganography is the science of concealing messages in other messages. Some historical techniques have involved invisible ink, subtle indentations in paper, and even tattooing messages under the hair of messengers. In this digital age, steganography provides means for hiding messages in digital audio files, in some kinds of images, and even for generating pseudo-English text which encodes the message.

Ideally, the original message is not noticeably degraded by presence of a hidden message. As a result, the most effective techniques tend to make use of data that contains a lot of redundancy, such as raw audio and image files. Steganography works much less effectively, if at all, with efficient compressed formats such as JPEG and MPEG.

Unfortunately, sending large amounts of raw audio and image data can arouse suspicion, and the pseudo-English encoding schemes are not sophisticated enough to fool a human observer. Stegimage is a program for embedding a mark(password) with an image and also for extracting the password from it

Concepts:

Embed:

This technique inserts the watermark(password in Ascii format) in the underused least signifcant bits(4 bits) of the image. This allows a watermark to be inserted in an image without affecting the value of the image. Typically, a color image consists of 3 color planes, Red, Green and Blue [RGB]. The blue plane was chosen as the location of the watermark since the human eye is less sensitive to changes in the blue

portion of the spectrum. Changes in this plane are less likely to be perceived by the viewer.

Extract:

This technique extracts the 4 LSB's of the pixel and combine to form the password

Each character requires two pixels to embed a charecter .

Compression

The compression scheme used by "Stegcompress" is a fairly rudimentary Huffman encoding scheme, where the tables are optimised for English text. This was chosen because the whitespace encoding scheme provides very limited storage space in some situations, and a compression algorithm with low overhead was needed. In other words, short messages had to compress to even shorter data. Depending on the text, you can usually get 25 - 40% compression.

If you want to compress a long message, or one not containing standard text, you would be better off compressing the message externally with a specialized compression program This usually results in a better compression ratio.

The Encoding Scheme

To show the beginning of a message, a tab is added immediately after the text on the first line where it will fit. This prevents the insertion of mail and news headers containing trailing spaces from corrupting the message, since a trailing tab must be found before extraction begins.

Data is written 3 bits at a time, coding for 0 to 7 spaces. Any messages not a multiple of 3 bits will be padded by zeroes. During extraction, an extra one or two bits at

the end will be ignored (fortunately there are no two-bit Huffman codes to confuse things).

An alternative scheme was considered, where bits were written one at a time as either a space or a tab. Although this scheme adds fewer characters per bit ,it requires more columns per bit and column space is the limiting factor.

Tabs are used to separate the blocks of spaces. Thus 3 bits are usually coded in 8 columns of text, and given that the default line length is 80 characters, this allows 30 bits to be stored on empty lines. A tab is not appended to the end of a line unless the last 3 bits coded to zero spaces, in which case it is needed to show some bits are actually there.

If a message will not fit into the available text, empty lines will be appended and used to contain the overflow. A warning message will also be produced, since this affects the look of the original text.

Options

Embed: Embed the message on the selected covertext

Extract: Extract the message hidden under the cover text by decoding the whitespaces and tabs

password - password for verification during extraction

line-length

When appending whitespace, "Stegimage" will always produce lines shorter than this value. By default it is set to 80.

Hidden_text

The contents of this string gets concealed in the selected cover text file.

PROC Stegimage()

BEGIN

Accept the password to embed in a photo

SWITCH(User's Choice)

CASE Load : Load the photo

CASE Embed: Embed the password

Masking the 4 LSB's of the pixels to 0 and OR the pixels with the first four pixels of the Ascii value of the character

CASE Submit: Call Login frame

Verify the password

END SWITCH

If (true)

Shows valid Frame

INPUT User's Choice

SWITCH(User's Choice)

CASE Create : Call PROC Steg1( )

CASE View : Call PROC Steg2( )

END SWITCH

ELSE

Call Invalid Frame

Cancel( )

END

"Steg 1" is a program for concealing messages in text files by appending tabs and spaces on the end of lines, and for extracting messages from files containing hidden messages. Tabs and spaces are

invisible to most text viewers, hence the steganographic nature of this encoding scheme.

The data is concealed in the text file by appending sequences of up to 7 spaces, interspersed with tabs. This usually allows 3 bits to be stored every 8 columns. An alternative encoding scheme, using alternating spaces and tabs to represent zeroes and ones, was rejected because, although it used fewer bytes, it required more columns per bit

The start of the data is indicated by an appended tab character, which allows the insertion of mail and news headers without corrupting the data.

"Stegcompress" provides rudimentary compression, using Huffman tables optimised for English text. However, if the data is not text, or if there is a lot of data, the use of the built-in compression is not recommended.

Whitespace Steganography

The encoding scheme used by "Stegencode" relies on the fact that spaces and tabs (known as *whitespace*), when appearing at the end of lines, are invisible when displayed in pretty well all text viewing programs. This allows messages to be hidden in ASCII text without affecting the text's visual representation. And since trailing spaces and tabs occasionally occur naturally, their existence should not be sufficient to immediately alert an observer who stumbles across them.

The "steg "program runs in two modes

Message concealment,

Message extraction.

During concealment, the following steps are taken.

Message -> Encoding-> Optional compression -> Concealment in text

Extraction reverses the process.

Extract data from text -> Decode-> Optional uncompression -> Message

```
PROC  Steg1( )
BEGIN

        INPUT User's Choice

                        SWITCH(User's Choice)
                        CASE Embed:  Call PROC Stegencode( )
                        CASE Load  : Call PROC LoadCovertext(
)
                        CASE    Save          :Call    PROC
SaveCovertext( )
                         END SWITCH
END


PROC Stegencode( )

     BEGIN

     Append the tabs and whitespaces
            Data is written 3 bits at a time, coding for 0 to 7 spaces
            This usually allows 3 bits to be stored in every 8 columns
     Call PROC StegCompress
     Call PROC Stegoutput
     END
```

PROC Stegcompress( )

BEGIN

Create a Huffman tables optimised for English text.

END

PROC Steg2( )

INPUT User's Choice

SWITCH(User's Choice)

CASE Extract: Call PROCStegencode(False)

CASE Load : Call PROC LoadCovertext( )

CASE Password : Accept the password

If(True)

Call Extract()

Else fail

END SWITCH

END

PROC Extarct( )

BEGIN

Decode the Whitespaces

Decompress the string to get the orginal message

Display the message in a hidden text area

END

PROC Stegencode( )

BEGIN

Append the tabs and whitespaces

Data is written 3 bits at a time, coding for 0 to 7 spaces

This usually allows 3 bits to be stored in every 8 columns

Call PROC StegCompress

Call PROC Stegoutput

END

RESULT

RESULT

The main results obtained with the implemented program are:

- Encoding and decoding of watermark are done The technique takes a very simple and straightforward approach to embedding the watermark. Bits of the image that are not normally noticed by the human eye are exploited to hide the watermark. works satisfactory
- to recognize own Identity photos and prevents duplication of photos;
- to enable identification of unauthorized copies made from watermarked photos
- Allows messages to be hidden in ASCII text without affecting the text's visual representation
- to save a file with the secret the message, it is effectively hidden from casual observers.
- to use files as a means to communicate concealed messages;

There exists a great potential for applications in many present day automated offices, where computational files rather than the traditional printed paper files are handled, and in electronic communications via Internet.

We presented the implementation of a system that is applicable to day-to-day situations in which "sufficient security" satisfies user needs because it discourages undue utilization of non-authorized documents.

Although the initial objective in this work was the use of watermarking to preserve author copyright and several other known functionalities of this technique, the developed application goes further, enabling a more flexible use that even includes steganography. It can be noted that this development has an important practical value and that it is feasible to market its utilization to the general public of word processor users, because it provides functions that are attractive for some, very useful for others and indispensable to the rest.

CONCLUSION

CONCLUSION

Finally, let us summarize the features of the project and give proposals for future work that would give continuity and would enhance the functionality of the application. With these suggestions, the project will turn conceptually more robust and applicable for enterprises.

Outstanding Features

Among the main features of the techniques presented here, the following aspects stand out as implementation novelties:

The best known application that implements steganography on text, hides one byte per text line and it can be easily detected. In this project, 3 bits are usually coded in
8 columns of text, and given that the default line length is 80 characters, this allows 30 bits to be stored on empty lines.

This work defines and implements other variants: character compression inserted in the internal code of the file

Concealed information stored is detected through a comparison with the password(ID photo) .

The techniques presented here are applicable to both pure watermarking and steganography, as well as to a combination of the two.

PROPOSALS FOR FUTURE WORK

The topic of Steganography & watermarking and in general protection of digital data will become increasingly important as more vendors wish to sell their digital works on the Internet. This includes all manner of digital data including books, music and movies.

The present software gives a basic picture of "Steganography" From the experience gained in the study of all these techniques, the state of the art, the possible applications and the perceived weaknesses, several roads appear for continuity of the work. They can be grouped into the following: This software deals only Ascii text as watermark. Images can be incorporated into this system instead of text.

Another improvement is ,here bits are inserted at the adjacent pixels, any one who came to know about this technique can easily decode the password, Hiding of the watermarking string could also be made more robust, by splitting up the string characters into different locations of the pixels and following different patterns, from values randomly obtained for each user.

Another functionality that can also be added is the distribution of the password by dispersing the charecters throughout the entire image, depending on the ratio of the quantity of pixels between the image utilized as channel and the password that we want to hide. This way, the search for out of normal formatting codes that could rise a reviewer's suspicion, would be hindered. Currently the password characters are

inserted one after another, beginning at the first available place for insertion.

To compress a long message, or one not containing standard text, Suggested to include externally with a specialized compression program, This usually results in a better compression ratio.

Encryption with the password can also be added , using the ICE encryption algorithm . Because of ICE's arbitrary key size, passwords of any length up to 1170 characters are supported (since only 7 bits of each character are used, keys up to 1024-bytes are supported).

REFERENCES

REFERENCES

Neil.F.Johnson and Sushil Jajodia

"Exploring Steganography:Seeing the Unseen"-IEEE Computer

Stephen Katzen Beisser , Fabian.A. Petticolas,

Information Hiding techniques for Steganography and Watermarking

W.Bender,D.Gruthi,and N.Morimoto (Feb 1995)

"Techniques for data hiding"

Patrick Naughton ,Herbert Schildt

The complete Reference Java 2 third Edition

Daniel Liang

Introduction to java programming

Paper by

Neil F. Johnson and Sushil Jajodia.

IEEEComputer,February1998:26-34.

R.J. Anderson, F.A.P. Petitcolas,

On the Limits of Steganography,

IEEE Journal on Special Areas in Communications v 16 no 4 (May98) 463-473.

Christopher G. Martin

Rochester Institute of Technology

Master of Science in Computer Science Thesis

Digital Image Watermarking Techniques

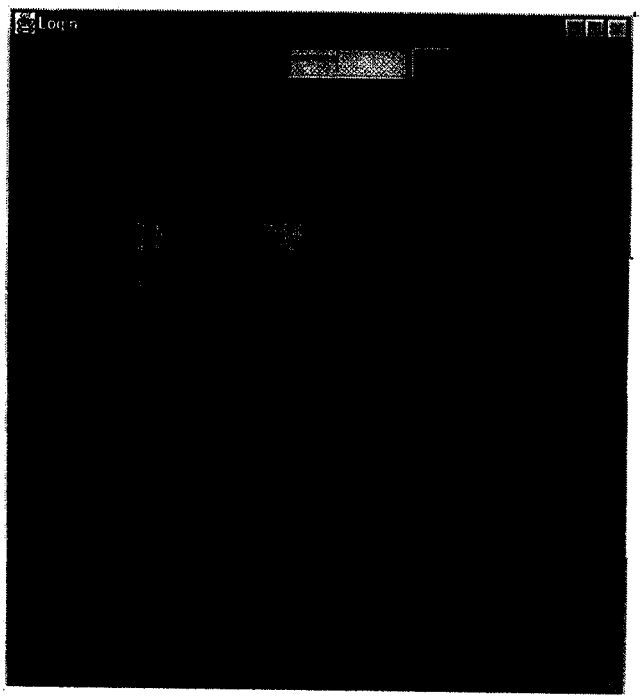
23 May 2000 - Document Revision 1.2

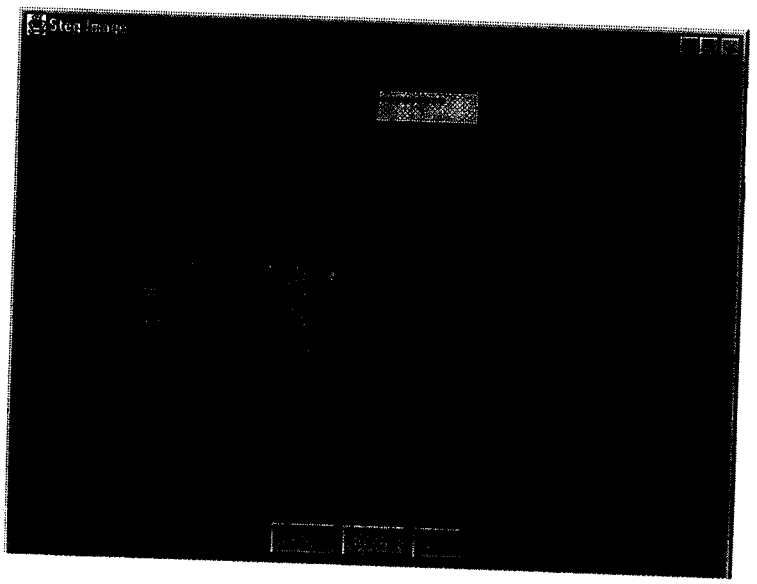
WWW.StegoArchive.com

WWW.Steganography.com

APPENDICES

OK :Verifies the password with the watermark (password)





Load: Load the image feom the file dialog box

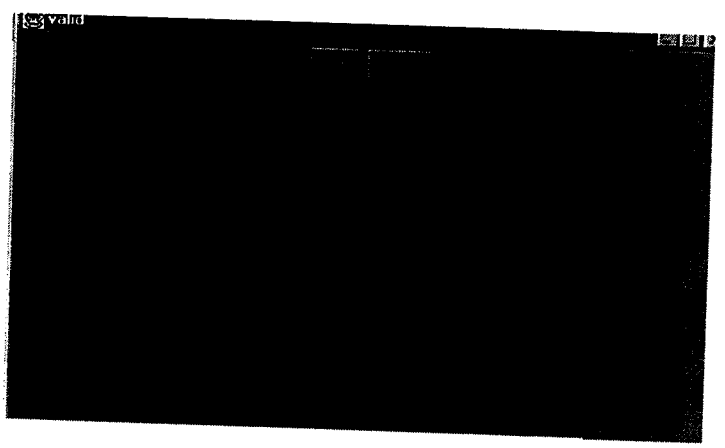
Password:Get the password

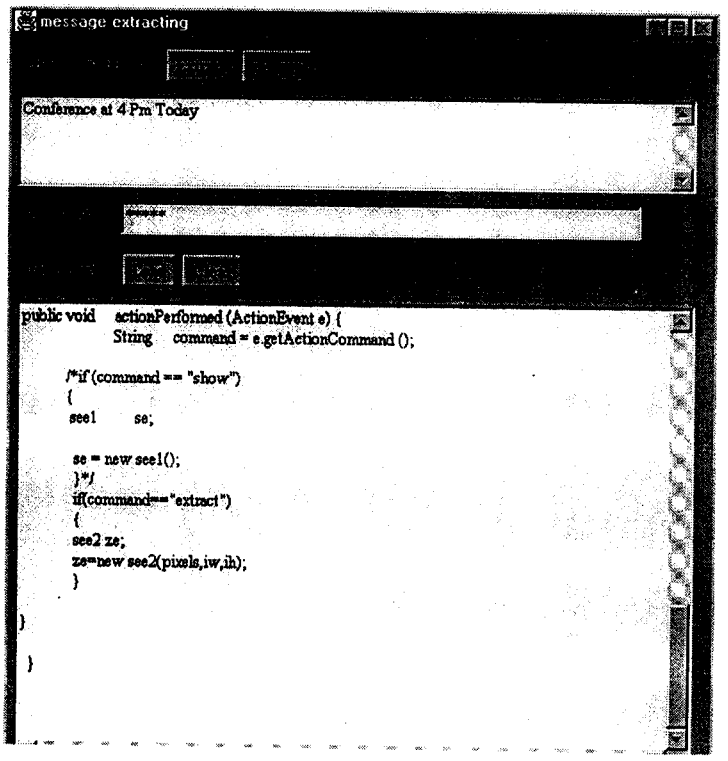
Embed:Embed the password in the photo

Submit: Opens the Login section

View : open the Extract Frame (Extracting the secret message)

Create: Open the Embed frame(Embedding the Secret message under the cover text)





Extract :Extract the Secret message from the covertext displayed on the text area

Load : To load the file

Password: Get the password for verification

Clear : Clear the text area